Federal Student Aid (FSA) Enterprise Portal Rollout – Release 1

Rules for Behavior

Every administrator and user should be made aware of their responsibilities for the use, protection, and release of sensitive Department of Education information under their control. In addition, those who administer, operate, or supervise the use or operation of the system must be aware of security and safety concerns specifically related to their efforts.

Each new user is a risk to the system and to other users of that system. Therefore, everyone should be versed in the rules of the system or acceptable behavior before being allowed to access the system.

Training should be tailored to the needs of the user and to the system security requirements. It is easier to abide by the rules if they are known and understood.

1. Assumptions

- Acceptable risk level can only be determined after security measures have been applied. Therefore any preliminary risk will change after evaluation of countermeasures.
- The security-relevant mechanisms, and characteristics of the system hardware and software are only a subset of system security safeguards. Security in itself is not the only driving force but a significant component that cannot be put asside.
- Nothing in this section consititutes authority to violate Federal, state, local or international law.

2. Rules

Effective security is a team effort involving participation and support of everyone. It is the responsibility of each user to know and follow these guidelines.

2.1. General Public

- Be aware that while there is a reasonable expectation of privacy, the equipment and the data it contains remains the properity of the Department of Education and authorized representatives may monitor the network for performance and auditing purposes.
- If you use this system, you should understand that all activities may be monitored and recorded. Anyone using this system expressly consents to such monitoring. WARNING -- If such monitoring reveals possible evidence of criminal activity, monitoring records may be provided to law enforcement officials.
- Passwords must remain private to ensure security.

2.2. Administration

- Only System Administrators will have logon privileges to servers.
- Appropriate Access Control Lists (ACL) shall be enforced.

3. Unacceptable Use

The follow are generally prohibited activities. Under no circumstances can an employee be exempted from violations of local, state, federal or international law.

- Revealing password or account details to others or allowing others to use the account without adhering to procedures.

- Accessing the network to gain or attempt to gain unauthorized access to data, system applications or other information or control that is not expressely authorised unless within the scope of duties. This includes disruption or attempted disruption of the network, user access or system controls.
- Executing any form of network monitoring that will intercept data not intended for the user affecting the activity unless authorized as part of the normal duties.
- Circumventing user authentication of any host, network or account.

4. Enforcement

At the immediate discretion of the System Security Officer, appropriate disciplinary action can be taken as one of the following:

- Verbal or electronic warning and demand to stop activity or provide satisfactory explanation.
- Monitoring of the activity for possible criminal or civil activity without notification.
- Termination of access after stating the violating activities.
- Immediate transfer of the violation to senior management or federal authorities for futher action. Such transfer may be with or without notification.

5. Sanctions

Sanctions may be imposed for whatever duration the System Security Officer determines provided management concurs.

Should the affected party wish to challenge the sanction, he/she must provide in writing through their supervisor to the System Security Officer the details and explanation of the incursion. Final decision of access will ultimately rest with the Chief Financial Officer, FSA.